

---

# OPTIMAL CURVES OF GENUS 1, 2 AND 3

by

Christophe Ritzenthaler

---

**Abstract.** — In this survey, we discuss the problem of the maximum number of points of curves of genus 1, 2 and 3 over finite fields.

**Résumé (Courbes optimales de genre 1, 2 et 3).** — Nous examinons la question du nombre maximum de points pour les courbes de genre 1, 2 et 3 sur les corps finis.

## 1. Introduction

The foundations of the theory of equations over finite fields were laid, among others, by mathematicians like Fermat, Euler, Gauss and Jacobi (see [Dic66]). Subsequently, there was little activity in the field at least until the end of the 19th century and the study of the zeta function of a curve. Initiated by Dedekind, Weber, Artin and Schmidt, this work led to an analogue of the Riemann hypothesis which was proved by Hasse in the case of elliptic curves and then by Weil in general in 1948 (see [Wei48]). The third, modern, period starts in 1980 with the work of Goppa [Gop77, Gop88]. His construction of error-correcting codes with good parameters from curves over finite fields renewed the interest in this theory.

With this application in mind, the theory has focused on the maximum number of points of a (projective, geometrically irreducible, non singular) curve of genus  $g$  over a finite field  $k = \mathbb{F}_q$ , denoted  $N_q(g)$ . Asymptotic results, *i.e.* values of  $N_q(g)/g$  when  $g$  goes to infinity and  $q$  is fixed, drew attention first, but Serre, in his lectures at Harvard [Ser85], gave equal treatment to the ‘dual’ case, *i.e.* values of  $N_q(g)$  when  $g$  is fixed and  $q$  varies. It quickly appeared that determining  $N_q(g)$  was a hard problem and as soon as  $g \geq 3$ , only sparse values are known (see for instance the web page [www.manypoints.org](http://www.manypoints.org) for the best estimates when  $q$  is small).

---

**2000 Mathematics Subject Classification.** — Primary 11G20, 11G10 Secondary 14K25, 14H45.

**Key words and phrases.** — optimal curve, isogeny class, indecomposable polarization, hermitian module, Serre’s obstruction, plane quartic, Siegel modular form, Hasse-Weil-Serre bound.

The author acknowledges partially supported by grant MTM2006-11391 from the Spanish MEC and by grant ANR-09-BLAN-0020-01 from the French ANR..

In this survey, we are going to describe the main ideas that have been developed to deal with the cases  $1 \leq g \leq 3$ . It is interesting to note that for each value of  $g$ , we will be confronted not only to harder computations but also to a completely new kind of issue. In order to emphasize this progression, we will not consider the actual value of  $N_q(g)$  but the following sub-problem. As we shall recall in Section 2.1,  $N_q(g) \leq 1 + q + g\lfloor 2\sqrt{q} \rfloor$  and we can wonder when  $N_q(g)$  reaches this bound. If it does, a curve with this number of points is called optimal and we are going to ask for which values of  $q$  such curves exist.

When  $g \leq 3$ , the classical game to prove or disprove the existence of optimal curves is

1. to prove the existence (or not) of an abelian variety  $A/k$  with a ‘good’ Weil polynomial (Section 2). This is going to control the number of points on a possible curve  $C/k$  such that  $\text{Jac } C \simeq A$ .
2. to put a good polarization  $a$  on  $A$  such that  $(A, a)/k$  is geometrically (*i.e.* over  $\bar{k}$ ) the Jacobian of a curve  $\bar{C}$  with its canonical polarization (Section 3).
3. to see if  $\bar{C}$  admits a model  $C/k$  such that  $(\text{Jac } C, j) \simeq (A, a)$  (where  $j$  is the canonical polarization of  $C$ ). We will see that if  $\bar{C}$  is non hyperelliptic, there can be an obstruction to this descent (see Section 4) and for  $g = 3$ , we will propose solutions to address the computation of the obstruction (see Section 5).

Most ideas we are going to present here are already contained in [Ser85] but our proofs for  $g = 1$  and 2 are sometimes different from the original ones and take advantage of subsequent simplifications of the theory.

**Conventions and notation.** In the following  $g \geq 1$  is an integer and  $q = p^n$  with  $p$  a prime and  $n > 0$  an integer. The letter  $k$  denotes the finite field  $\mathbb{F}_q$  and  $K$  any perfect field. When we speak about a *genus  $g$  curve* we mean that the curve is projective, geometrically irreducible and non-singular. If  $A$  and  $B$  are varieties over a field  $K$ , when we speak of a morphism from  $A$  to  $B$  we always mean a morphism *defined over  $K$* . So, for instance  $\text{End}(A)$  is the ring of endomorphisms defined over  $K$ ,  $A \sim B$  means  $A$  isogenous to  $B$  over  $K$ , etc. If  $(A, a)$  and  $(B, b)$  are polarized abelian varieties, by an isomorphism between them, we always mean ‘as polarized abelian varieties’.

**Acknowledgements.** I would like to thank Christian Maire for suggesting me to write this survey. This is part of my ‘habilitation’ thesis [Rit09] which was defended during the workshop Theory of Numbers and Applications which was organized by Karim Belabas and Christian Maire in Luminy in December 2009. I am really grateful to Detlev Hoffmann for the references of Remark 3.5 and to the Number Theory List community and particularly to Samir Siksek for helping me with Remark 3.10.

## 2. Control of the isogeny class

**2.1. Bounds.** — Let  $C/k$  be a genus  $g$  curve. We recall that its *Weil polynomial*  $\chi_C$  is the Weil polynomial of  $\text{Jac } C/k$ , *i.e.* the characteristic polynomial of the action of the  $k$ -Frobenius endomorphism on an  $\ell$ -adic Tate module for any prime  $\ell \neq p$ . It is well known that it can be

written

$$\chi_C = \prod_{i=1}^g (X^2 + x_i X + q) \in \mathbb{Z}[X]$$

with  $x_i \in \mathbb{R}$  and  $|x_i| \leq 2\sqrt{q}$ . Since

$$\#C(k) = q + 1 + \sum_{i=1}^g x_i,$$

it is clear that  $\#C(k) \leq 1 + q + \lfloor 2g\sqrt{q} \rfloor$ , which is known as *Hasse-Weil bound* [Wei48] and so  $N_q(g)$  is less than this bound too. It is possible to improve this bound as the following lemma shows.

**Lemma 2.1 (Hasse-Weil-Serre bound [Ser83b]).** — *Let  $m = \lfloor 2\sqrt{q} \rfloor$ . Then*

$$N_q(g) \leq 1 + q + gm.$$

*Proof.* — It is enough to use the arithmetic-geometric mean inequality:

$$\frac{1}{g} \sum_{i=1}^g (m + 1 - x_i) \geq \left( \prod_{i=1}^g (m + 1 - x_i) \right)^{1/g} \geq 1,$$

the last inequality coming from the fact that the product is a non-zero integer.  $\square$

This motivates us to give the following definition.

**Definition 2.2.** — We say that a genus  $g$  curve  $C/\mathbb{F}_q$  is *optimal* if

$$\#C(\mathbb{F}_q) = q + 1 + gm.$$

In that case  $N_q(g) = q + 1 + gm$ .

Note that the previous definition is not universally accepted. Some authors call *maximal* (or  $\mathbb{F}_q$ -maximal) what we call optimal by reference to the historical cases with  $n$  even and  $N_q(g) = q + 1 + gm$ . We prefer to keep the word maximal for curves which numbers of points is equal to  $N_q(g)$  and our terminology is coherent with the historical one as well.

**Remark 2.3.** — If  $g \geq (q - \sqrt{q})/2$ , the bound can be improved, thanks to the *explicit methods* of Oesterlé (and is known as *Oesterlé bound* [Ser83b]). It uses the fact that the number of places of each degree on the curve is non negative. As we will mainly deal with small values of  $g$  compared to  $q$ , the Hasse-Weil-Serre bound will be our reference.

**2.2. Existence of the isogeny class.** — Equality in the arithmetic-geometric mean inequality is equivalent to the fact that all terms in the sum are equal and so  $x_i = m$  for all  $1 \leq i \leq g$ . Hence, if an optimal curve  $C$  exists, its Weil polynomial has the particular simple expression

$$\chi_C = (X^2 + mX + q)^g.$$

Honda-Tate theory as explained in [Tat66], [Hon68], [Wat69], [MW71] or [Tat71] shows that if  $p \nmid m$  (resp.  $n$  is even) then  $\text{Jac } C$  is isogenous to  $E^g$  where  $E$  is an ordinary (resp. supersingular) elliptic curve with trace  $-m$ . However, if  $p|m$  and  $n$  is odd, this might not be true (see the proof of Proposition 2.5 below) and there is for instance a simple abelian variety

of dimension 9 over  $\mathbb{F}_{5^9}$  with such Weil polynomial. If we restrict to  $g \leq 3$ , it can be proved that this never happens (see for instance the proof of Corollary 4.2 of [NR10]).

**Lemma 2.4.** — *If  $C/\mathbb{F}_q$  is an optimal curve of genus  $g \leq 3$  then  $\text{Jac } C$  is isogenous to  $E^g$  where  $E$  is an elliptic curve of trace  $-m$ .*

The first necessary condition is then to see whether such an elliptic curve exists or not.

**Proposition 2.5 (Deuring [Deu41]).** — *There does not exist an elliptic curve with trace  $-m$  if and only if  $n \geq 3$ ,  $n$  is odd and  $p|m$ .*

*Proof.* — Let  $F = X^2 + mX + q$ . Since  $m < 2\sqrt{q}$  if and only if  $q$  is not a square,  $F$  is irreducible over  $\mathbb{Q}$  when  $n$  is odd and  $F = (X + \sqrt{q})^2$  when  $n$  is even.

If  $n$  is odd, by [Wat69, p.527], the minimal  $e$  for which  $\chi = F^e$  is the Weil polynomial of an abelian variety of dimension  $e$  over  $k$  is the least common denominator of  $v_p(F_\nu(0))/n$  where  $F_\nu$  denotes the factors of  $F$  in  $\mathbb{Q}_p[t]$  and  $v_p$  the  $p$ -adic valuation of  $\mathbb{Q}_p$ . Hence  $F$  is the Weil polynomial of an elliptic curve if and only if  $n|v_p(F_\nu(0))$  for all factors. This is of course satisfied if  $n = 1$ . Looking at the Newton polygon of  $F$ , we see that if  $p \nmid m$  then  $v_p(F_\nu(0)) = n$  or 0, so  $e = 1$ . With the same technique, if  $n > 1$  odd and  $p|m$ , then  $v_p(F_\nu(0)) < n$  and so  $e > 1$ .

If  $n$  is even, we apply the previous arguments to  $F = X + \sqrt{q}$ . Since  $v_p(\sqrt{q})/n = 1/2$ ,  $e = 2$  so  $F^2 = X^2 + mX + q$  is the Weil polynomial of an elliptic curve.  $\square$

Actually, the only values of  $q = p$  for which  $p|m$  are  $q = 2$  or  $q = 3$ .

**Remark 2.6.** — For any value of  $-m \leq t \leq m$ , one knows if an elliptic curve with trace  $t$  exists (see [Wat69, Th.4.1]). Also, the possible Weil polynomials of the isogeny classes of abelian surfaces (resp. threefolds) can be found in [MN02, Lem.2.1,Th.2.9] (resp. [Xin96, Hal10]).

### 3. Existence of an indecomposable principal polarization

The Jacobian of a genus  $g$  curve  $C/K$  is naturally equipped with a *principal polarization*  $j$  induced by the intersection pairing on the curve  $C$ . Since the theta divisor  $\text{Sym}^{g-1} C \hookrightarrow \text{Jac } C$  associated to  $j$  is geometrically irreducible,  $(\text{Jac } C, j)$  is geometrically *indecomposable*, i.e. there does not exist an abelian subvariety  $B \subset \text{Jac } C$  defined over  $\bar{K}$  such that  $j$  induces on  $B$  a principal polarization. Conversely, starting with  $A = E^g$  where  $E$  is an elliptic curve, it is clear that  $A$  always admits a principal polarization  $a_0$  given by the product of the principal polarizations on each factor. As  $a_0$  is decomposable,  $(A, a_0)$  is not (even geometrically) a Jacobian. Hence ‘good’ principal polarizations on  $A$  (or on abelian varieties in the isogeny class of  $A$ ) have to be more subtle. Luckily, equivalences of category have been developed to translate the existence of an indecomposable polarization into the existence of purely algebraic objects. As far as I know several points of view co-exist and it is not clear to see how to go from one to the other. I shall use Serre’s one and mention others in remark.

**Remark 3.1.** — Howe [How95],[How96] has developed a powerful machinery to prove the existence of a principally polarized abelian variety in the isogeny class of an abelian variety  $A/k$ . But only when  $A$  is simple, it is easy to see that the polarization is indecomposable (see

[Ryb08] for the case  $E \times B$  where  $E$  is an elliptic curve and  $B$  a geometrically simple abelian surface).

**3.1. The equivalences.** — Let us start with  $E$  ordinary. Let  $E/k$  be an ordinary elliptic curve with trace  $t$ . If  $\pi$  denotes the  $\mathbb{F}_q$ -Frobenius endomorphism of the curve  $E$ , then the ring  $R := \mathbb{Z}[X]/(X^2 - tX + q)$  is isomorphic to  $\mathbb{Z}[\pi] \subset \text{End}(E)$ . Serre [Ser85, Se.50-53], [Lau02, Appendix] defines an equivalence of category  $T$  between the category of abelian varieties which are isogenous to a power of  $E$  and  $R$ -modules of finite type without torsion. The functor  $T$  maps an object  $A$  to the  $R$ -module  $L = \text{Hom}(E, A)$ . Obviously, the rank of  $L$  is equal to the dimension of  $A$ . This functor also behaves nicely with respect to duality: if we denote  $\hat{L}$  the ring of anti-linear homomorphism  $f : L \rightarrow R$  (i.e.  $f(rx) = \bar{r}f(x)$  for all  $r \in R$  and  $x \in L$ ) then  $T(\hat{A}) = \hat{L}$ . Thus a morphism  $a : A \rightarrow \hat{A}$  defines a morphism  $h : L \rightarrow \hat{L}$  and hence an hermitian form  $H : L \times L \rightarrow R$ . Serre proves that  $a$  is a polarization if and only if  $H$  is positive definite, that  $a$  is principal if  $(L, H)$  is *unimodular* (i.e.  $h(L) = \hat{L}$ ) and moreover (geometrically) indecomposable if and only if  $(L, H)$  is *indecomposable*, i.e. cannot be written as a sum of orthogonal sub-modules. The couple  $(L, H)$  is called a *hermitian module*.

**Remark 3.2.** — This equivalence is inspired by the classical theory over  $\mathbb{C}$ , which is not surprising since ordinary abelian varieties can be lifted canonically and this is used in [Del69]. When  $A = E^g$  and  $\text{End}(E) \simeq R$ , a more explicit point of view can be considered looking at the hermitian matrix  $M := a_0^{-1}a \in \text{End}(A) = M_g(\text{End}(E)) \simeq M_g(R)$  (see [Rit10], [Lan06]). For  $g = 2$ , Kani's construction [Kan97] also gives necessary and sufficient conditions for 'gluing' two elliptic curves along their  $n$ -torsion for  $n > 1$ . Both points of view are related by the Cholewsky decomposition of  $M$ .

A classification of rank 2 and 3 hermitian modules was achieved in [Hof91, Th.8.1,8.2] (see also [Sch98] for further computations) and translates into the following result.

**Proposition 3.3.** — *Let  $E$  be an ordinary elliptic curve with trace  $t$ . There is no abelian surface (resp. threefold) with a geometrically indecomposable principal polarization in the class of  $E^2$  (resp.  $E^3$ ) if and only if  $t^2 - 4q \in \{-3, -4, -7\}$  (resp.  $t^2 - 4q \in \{-3, -4, -8, -11\}$ ).*

**Remark 3.4.** — For  $g = 2$ , the result can be traced back to [HN65, p.14], where the authors prove the existence of genus 2 curves which Jacobian is *isomorphic* to  $E^2$  by constructing free indecomposable hermitian modules (in [Hay68], the precise number of isomorphism classes of such curves is computed). For  $g = 2$  or 3, it could also be deduced from the mass formulae (i.e. number of weighted classes by the order of their automorphism group) of [HK86, HK89] (although, according to Hoffmann (*loc. cit.* p.400) there is a minor mistake in these computations).

**Remark 3.5.** — For  $g > 3$ , there have been several partial answers on the existence of indecomposable unimodular positive definite hermitian modules of rank  $g$  over the ring of integers of an imaginary quadratic field  $\mathbb{Q}(\sqrt{-d})$ . It seems that in [Zhu97] and [WL01] a complete answer is given: there always exists one, except when  $d = 1$  and  $g = 5$  or  $d = 3$  and  $g = 4, 5, 7$ . One should be careful since, according to the Mathscinet review of [Zhu97] by Hoffmann, the proofs contain several mistakes. Also, I do not know if the case of non maximal orders has been considered.

Assume now that  $E$  is supersingular. More precisely, let  $E/\mathbb{F}_p$  be an elliptic curve with trace 0, so that  $E$  is supersingular, all the geometric automorphisms of  $E$  are defined over  $\mathbb{F}_{p^2}$  and  $\text{Tr}(E/\mathbb{F}_{p^2}) = -2p = -m$ . One says that an abelian variety  $A$  (resp. a curve  $C$ ) is *superspecial* if  $A$  (resp.  $\text{Jac } C$ ) is geometrically isomorphic to a product of supersingular elliptic curves. A result of Deligne (see [Shi79, Th.3.5]) shows that when  $g > 1$ , a superspecial abelian variety of dimension  $g$  is geometrically isomorphic to  $E^g$  (whereas for  $g = 1$  there are non-isomorphic supersingular elliptic curves as soon as  $p > 7$ ). However, the description of the isogeny class is made more complicated than in the ordinary case by the existence of ‘continuous’ families of isogenies. For instance, already when  $g = 2$  (see [Oor75]), a supersingular abelian surface is either geometrically isomorphic to  $E^2$  (and so superspecial) or of the form  $E^2/\alpha_p$  where  $\alpha_p$  is the unique local-local group scheme over  $\mathbb{F}_p$ , the injection of  $\alpha_p$  in  $E^2$  being parametrized by  $\mathbb{P}^1(\overline{\mathbb{F}}_p) \setminus \mathbb{P}^1(\mathbb{F}_{p^2})$ . In the latter, it can be shown that  $A$  is not superspecial and the description of the polarizations on this object is more evolved. For this reason, we will concentrate only on existence results and limit ourselves to the superspecial case.

**Remark 3.6.** — Note that it is still possible to obtain a complete description for  $g = 2$  in the non-superspecial case like in [IKO86] or [HNR09, Part.2] where the mass formula of [Ibu89] were used.

As in Remark 3.2, we describe the polarizations on  $A = E^g$  by matrices  $M := a_0^{-1}a$  in  $\text{End}(A) = \text{M}_g(\text{End}(E))$ . Now,  $\text{End}(E)$  is a quaternion algebra, so we need results on the number  $n_g$  of *positive definite quaternion hermitian forms*. Then, to obtain the number of (geometrically) indecomposable polarizations on  $E^g$ , the idea is to subtract to  $n_g$  the number of polarizations coming from combinations of lower dimensional abelian varieties. In this way, one gets

**Proposition 3.7** ([Eke87, Prop.7.5]). — *There is no geometrically indecomposable principal polarization on  $E^g$  if and only if  $g = 2$  and  $p = 2$  or 3, or  $g = 3$  and  $p = 2$ .*

**Remark 3.8.** — More precisely, Ekedahl gives in [Eke87, Prop.7.2] the mass of indecomposable principal polarizations on  $E^g$ . However, Brock [Bro93, Th.3.10.c] corrects a mistake in the case  $g = 3$ . He also completes and recovers several results obtained in [HI83, I], [KO87] for  $g = 2$  and in [Has83], [Oor91] for  $g = 3$ . For instance, in [Bro93, Th.3.14, Th.3.15], he gives the number of genus 2 and genus 3 superspecial curves for each possible group of automorphisms.

**3.2. Application.** — We can now answer the question of the existence of a good polarization when  $g \leq 3$ .

**Theorem 3.9.** — *Let  $E$  be an elliptic curve with trace  $-m$ . There is no abelian surface (resp. threefold) with a geometrically indecomposable principal polarization in the isogeny class of  $E^2$  (resp.  $E^3$ ) if and only if  $q = 4$  or 9 or  $m^2 - 4q \in \{-3, -4, -7\}$  (resp.  $q = 4$  or 16 or  $m^2 - 4q \in \{-3, -4, -8, -11\}$ ).*

*Proof.* — When  $p \nmid m$ ,  $E$  is ordinary so we can use Proposition 3.3.

When  $n$  is odd and  $p|m$ ,  $E$  exists if and only if  $q = 2$  or 3, which leaves these two cases to be treated apart (for instance by extensive computer research of curves using Theorem 4 or by

Remark 3.10).

When  $n$  is even then  $p|m$ . We distinguish several cases.

- When  $p > 3$  and  $g = 2$  (resp.  $p > 2$  and  $g = 3$ ), Proposition 3.7 shows that there is always an indecomposable principal polarization on  $E^2$  (resp.  $E^3$ ). Note that when  $4|n$ , the present  $E$  is the quadratic twist of the elliptic curve in Proposition 3.7.
- When  $p = 2$  and  $g = 2$ , explicit constructions as in [MN07] or a ‘gluing’ argument as in [Ser85, Se.32], [Sha01, Prop.30] shows that one can get a curve  $C/\mathbb{F}_{2^n}$  such that  $\text{Jac } C$  is isogenous to  $E^2$  as soon as  $n > 2$ .
- When  $p = 2$ ,  $g = 3$  and  $n > 4$ , An explicit non hyperelliptic curve  $C/\mathbb{F}_{2^n}$  such that  $\text{Jac } C \sim E^3$  can be constructed. (see [Rit09, Lem.2.3.8]). Note that in [NR08], the more general question of the existence of a Jacobian in the isogeny class of a supersingular abelian threefold in characteristic 2 is addressed.
- Finally when  $p = 3$  and  $g = 2$ , one can find an explicit construction in [Kuh88] (see also [Sha01, Cor.37] where a mistake is corrected) as soon as  $n > 2$ . This work was also generalized to all supersingular abelian surfaces in characteristic 3 in [How08].

□

**Remark 3.10.** — The cases  $m^2 - 4q \in \{-3, -4\}$  can also be excluded thanks to a proof due to Beauville [Sha01, Th.16], [Ser85, Se.13] without any hypothesis on the  $p$ -rank of  $E$  (and then  $q = 2, 3$  are covered).

As conjecturally, there is infinitely many  $p$  in the forms  $p = x^2 + 1$  and  $p = x^2 + x + 1$  the equations  $m^2 - 4p^n \in \{-3, -4\}$  have infinitely many solutions with  $n = 1$ . For  $n > 1$  odd, one knows that the set of solutions is finite. For instance, in [Ser83a], we find that there is only one solution to the equation  $q = x^2 + x + 1$  namely  $q = 7^3$  and none to  $q = x^2 + 1$ .

Similarly, the case of discriminant  $-7$  corresponds to the equation  $q = x^2 + x + 2$  with unique solutions  $q \in \{2^3, 2^5, 2^{13}\}$  when  $n > 1$  is odd.

The case of discriminant  $-8$  corresponds to  $q = x^2 + 2$ , which, when  $n > 1$  is odd, has  $q = 3^3$  for unique solution. This is proved using the same arguments as the last case below.

Finally, the case of discriminant  $-11$  corresponds to  $q = x^2 + x + 3$ . When  $n > 1$  is odd,  $q = 3^5$  is the unique solution thanks to the following argument due to Samir Siksek. The equation can be rewritten  $(2x + 1)^2 + 11 = 4p^n$  and factors in  $K = \mathbb{Q}(\sqrt{-11})$  as

$$\left( \frac{2x + 1 + \sqrt{-11}}{2} \right) \left( \frac{2x + 1 - \sqrt{-11}}{2} \right) = p^n.$$

Since  $n$  is odd and  $\mathcal{O}_K$  is a principal domain, there exists  $\alpha = (a + b\sqrt{-11})/2 \in \mathcal{O}_K$  such that  $\alpha^n = (2x + 1 + \sqrt{-11})/2$  and  $\alpha\beta = p$  with  $\beta = \bar{\alpha}$ . Now, note that  $\alpha^n - \beta^n = \sqrt{-11}$  and since  $(\alpha^n - \beta^n)/(\alpha - \beta) = 1/b \in \mathcal{O}_K$ , we see that  $b = \pm 1$ . Hence, if we fix  $n$ , we can find the finite set of integer solutions of this polynomial equation in  $a$ . However, to solve it for all  $n$  we have to invoke the much deeper theorem from [BHV01] which tells us that if there is a solution then  $n < 4$ ,  $n = 5$  or  $n = 12$ . Indeed, with the terminology and notation of *loc. cit.*, one sees that  $u_n = (\alpha^n - \beta^n)/(\alpha - \beta) = \pm 1$  is a Lucas number without primitive divisor, so the Lucas pair  $(\alpha, \beta)$  is  $n$ -defective.

#### 4. Optimal curves

As we have seen in Section 3, the strategy we have applied so far works in any dimension. If we now have to restrict ourselves to the dimensions less than or equal to 3 is because, in these cases, the condition ‘has an indecomposable principal polarization’ is geometrically sufficient to be the Jacobian of a curve. This is not true when the dimension is bigger, as it is proved simply by noting that the dimension of the moduli space of curves of genus  $g$ ,  $3g - 3$ , is less than the dimension of the moduli space of principally polarized abelian varieties of dimension  $g$ ,  $g(g + 1)/2$ . However,

**Proposition 4.1 ([OU73]).** — *For  $g \leq 3$ , any geometrically indecomposable principally polarized abelian variety  $(A, a)/K$  is the Jacobian of a curve  $\bar{C}$  over  $\bar{K}$ .*

So, given  $(A, a)/K$  as in Proposition 4.1, the question boils down to know whether one can descend the curve  $\bar{C}$  to a curve  $C$  over  $K$  such that  $(\text{Jac } C, j) \simeq (A, a)$ . Surprisingly the answer is ‘not always’.

**Theorem 4.2 (Arithmetic Torelli theorem).** — *There is a unique model  $C/K$  of  $\bar{C}$  such that:*

1. *If  $\bar{C}$  is hyperelliptic, there is an isomorphism*

$$(\text{Jac } C, j) \xrightarrow{\sim} (A, a).$$

2. *If  $\bar{C}$  is not hyperelliptic, there is a unique quadratic character  $\varepsilon$  of  $\text{Gal}(\bar{K}/K)$ , and an isomorphism*

$$(\text{Jac } C, j) \xrightarrow{\sim} (A, a)_\varepsilon$$

*where  $(A, a)_\varepsilon$  is the quadratic twist of  $A$  by  $\varepsilon$ .*

**Remark 4.3.** — It is tricky to find the right origin of the previous result. In [Ser85, Se.69], Gouvêa indicates ‘Oort + ...’ as a reference. One can indeed find in [Oor91, Lem.5.7] a similar result (but this is 1991). Sekiguchi also worked on this question but after two errata, he gives in [Sek86] only the existence of the model  $C/K$  but does not speak about  $\varepsilon$ . One can also find this result in [Maz86, p.236].

The notation  $(A, a)_\varepsilon = (A_\varepsilon, a_\varepsilon)$  should be understood as follows. The variety  $A_\varepsilon$  is uniquely defined up to isomorphism by the following property: there exists a quadratic extension  $L/K$  and an isomorphism  $\phi : A \rightarrow A_\varepsilon$  defined over  $L$  such that for all  $\sigma \in \text{Gal}(\bar{K}/K)$  one has  $\phi^\sigma = \varepsilon(\sigma)\phi$ . The polarization  $a_\varepsilon$  is the pull-back of  $a$  by  $\phi^{-1}$ .

This result is a consequence of Weil’s descent as explained in [Ser68, 4.20] and of Torelli theorem [Mat58, p.790-792]. The schism which appears between the hyperelliptic and non hyperelliptic case is due to the fact that

$$\text{Aut}(\text{Jac } C, j) \simeq \begin{cases} \text{Aut}(C) & \text{if } C \text{ is hyperelliptic,} \\ \text{Aut}(C) \times \{\pm 1\} & \text{if } C \text{ is non hyperelliptic.} \end{cases}$$

**Definition 4.4.** — The character  $\varepsilon$  (or the discriminant of the extension  $L/K$ ) is called *Serre’s obstruction*. By extension, in the hyperelliptic case, we say that  $\varepsilon$  is trivial.



Let us emphasize why this obstruction is an issue in our strategy. So far we have been able to prove in certain cases the existence of a geometrically indecomposable principally polarized abelian variety  $(A, a)/k$  with Weil polynomial  $(X^2 + mX + q)^g$ . Thanks to Proposition 4.1, we know that it is geometrically the Jacobian of a curve  $\bar{C}$ . If the obstruction is trivial, then  $\bar{C}$  descends to a curve  $C/k$  such that  $\text{Jac } C \simeq A$  and so  $C$  is optimal. On the contrary, if the obstruction is not trivial, then  $\bar{C}$  descends to a curve  $C/k$  such that  $\text{Jac } C$  is isomorphic to the (unique) quadratic twist of  $A$  and so its Weil polynomial is  $(X^2 - mX + q)^g$ . In particular  $\#C(k) = q + 1 - gm$  and  $C$  is not optimal (and actually  $C$  has the minimum number of points a genus  $g$  curve over  $k$  can have).

**4.1. The end of the genus 1 and 2 cases.** — Since a genus 1 curve over a finite field always has a rational point, it is an elliptic curve and Proposition 2.5 tells us when an optimal genus 1 curve exists (for the value of  $N_q(1)$  see [Deu41] or [Ser83a]). When  $g = 2$ , all genus 2 curves are hyperelliptic so the obstruction is always trivial and the result is similar to Theorem 3.9, namely

**Theorem 4.5 (Serre).** — *There is no optimal curve of genus 2 over  $\mathbb{F}_q$  if and only if  $q = 4$  or 9 or  $m^2 - 4q \in \{-3, -4, -7\}$ .*

In [Ser83a], a closed formula for the value of  $N_q(2)$  is given. More recently, completing the work started by many authors, we obtained in [HNR09] the complete picture for abelian surfaces, *i.e.* we determined which isogeny classes contain the Jacobian of a genus 2 curves in terms of the coefficients of the Weil polynomial.

## 5. The genus 3 case

As there exist non hyperelliptic genus 3 curves (the non-singular plane quartics), Serre's obstruction may not be trivial. One hope is that, for each  $q$ , there would be an optimal *hyperelliptic* curve but this possibility has to be discarded: for instance, there does not exist any optimal hyperelliptic genus 3 curves over  $\mathbb{F}_{2^n}$  with  $n$  even since supersingular hyperelliptic curves do not exist in characteristic 2 [Oor91]. Other counterexamples can be found in odd characteristic as well as it will be apparent in Proposition 5.6. Therefore, it is important to be able to compute Serre's obstruction. Currently, there is no perfect solution to this problem but we will summarize some of the ideas and partial answers which have been obtained.

**5.1. Special families.** — The key-idea is to use some families of curves with non trivial automorphisms, such that their Jacobian is a product of elliptic curves explicitly obtained as quotient by certain automorphism subgroups. Then one tries to reverse the process and see if one can glue given elliptic curves together to get a curve in the family. The possible quadratic extension one has to make during the construction is Serre's obstruction. Let us illustrate this procedure with an example.

**Example 5.1.** — The following family represents genus 3 non hyperelliptic curves in characteristic 2 with automorphism group containing  $(\mathbb{Z}/2\mathbb{Z})^2$

$$C : (a(x^2 + y^2) + cz^2 + xy + ez(x + y))^2 = xyz(x + y + z), \quad ac(a + c + e) \neq 0.$$

The involutions are  $(x : y : z)$  maps to  $(y : x : z)$ ,  $(x + z : y + z : z)$  or  $(y + z : x + z : z)$ . To get the equation of the curve  $E_1 = C / \langle (x : y : z) \mapsto (y : x : z) \rangle$ , one introduces the invariant functions  $X = x + y$ ,  $Y = xy$  and finds

$$E_1 : (aX^2 + c + Y + eX)^2 = Y(X + 1).$$

Doing similarly with the other involutions and rewriting the equations of the elliptic curves (see [NR10] for details) one gets that  $\text{Jac } C \sim E_1 \times E_2 \times E_3$  where

$$\begin{aligned} E_1 & : y^2 + xy = x^3 + ex^2 + a^2(a + c + e)^2, \\ E_2 & : y^2 + xy = x^3 + ex^2 + c^2(a + c + e)^2, \\ E_3 & : y^2 + xy = x^3 + ex^2 + c^2a^2. \end{aligned}$$

Conversely, we now want to glue ordinary elliptic curves  $E_i$  with  $j$ -invariant  $j_i \neq 0$ . They can always be written  $E_i : y^2 + xy = x^3 + ex^2 + 1/j_i$  where, if  $q > 2$ ,  $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(e) = 0$  if and only if  $\text{Tr}(E_i) \equiv 1 \pmod{4}$ . Let  $s_i^4 = 1/j_i$ , then

$$\begin{aligned} a &= \frac{s_1 s_3}{s_2}, \\ c &= \frac{s_2 s_3}{s_1}, \\ (1) \quad e &= \frac{s_1 s_3}{s_2} + \frac{s_2 s_3}{s_1} + \frac{s_1 s_2}{s_3}. \end{aligned}$$

Now, for instance, assume that  $m \equiv -1 \pmod{8}$ . This happens for  $n = 35, 37, 63, \dots$ . We choose  $E = E_1 = E_2 = E_3$  an ordinary elliptic curve with trace  $-m$  and  $j$ -invariant  $j$  ( $E$  exists since  $2 \nmid m$ ). Since we can assume that  $q > 4$ , the curve  $E$  has an 8-torsion point and it is not difficult to check that this implies (actually is equivalent to)  $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2} 1/j = 0$ . Hence

$$\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2} \left( \frac{s_1 s_3}{s_2} + \frac{s_2 s_3}{s_1} + \frac{s_1 s_2}{s_3} \right) = \text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(1/j) = 0.$$

On the other hand, since  $\text{Tr}(E) \equiv 1 \pmod{4}$ , we have  $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(e) = 0$  as well, so there is no obstruction to (1). Actually, we get an explicit equation

$$C : (j^{-1/4}(x^2 + y^2 + z^2 + xz + yz) + xy)^2 = xyz(x + y + z)$$

for the optimal curve.

Exploiting other families of curves in characteristic 2, we get the following result.

**Theorem 5.2** ([NR08, NR10]). — *If  $n$  is even, there exists an optimal curve over  $\mathbb{F}_{2^n}$  if and only if  $n \geq 6$ .*

*If  $n$  is odd and  $m \equiv 1, 5, 7 \pmod{8}$ , there is an optimal curve over  $\mathbb{F}_{2^n}$ .*

When  $n > 1$  is odd and  $m$  is even, there is of course no optimal curve since there is no elliptic curve with trace  $-m$ . So only the case  $m \equiv 3 \pmod{8}$  is missing to get a complete answer when  $p = 2$ .

More recently, Mestre [Mes10] has worked with a family of curves with automorphism group  $S_3$  and showed that if  $p = 3$  (resp.  $p = 7$ ),  $3 \nmid m$  (resp.  $3 \mid m$ ) and  $-m$  is a non-zero square modulo 7 (resp.  $n \geq 7$ ), then there exists an optimal curve over  $\mathbb{F}_{3^n}$  (resp.  $\mathbb{F}_{7^n}$ ).

To conclude on this approach, let us point out that one could use the family with automorphism group  $(\mathbb{Z}/2\mathbb{Z})^2$  (called *Ciani quartics*) also in characteristic greater than 2, since Serre's obstruction has been worked out in [HLP00]. Unfortunately, one does not see when this obstruction is trivial knowing only  $m$  (one needs the equations of the elliptic factors to decide).

**5.2. Serre's analytic strategy.** — Inspired by results of Klein [Kle90, Eq.118,p.462] and Igusa [Igu67, Lem.10,11], in a 2003 letter to Jaap Top [LR08], Serre stated a strategy to compute the obstruction when the characteristic is different from 2. Roughly speaking, his idea was that a certain Siegel modular form evaluated at a 'moduli point'  $(A, a)/K$  is a square in  $K$  if and only if the obstruction is trivial. In a series of three papers, it was shown that this is accurate (first for Ciani quartics, then in general) and how to compute the obstruction in the case of the power of a CM elliptic curve. Let us state the general result without any comments on the proof which would lead us too far from our initial purpose (see however [Rit09, Chap.4] for details).

**Theorem 5.3 ([LRZ10]).** — *Let  $A = (A, a)/K$  be a principally polarized abelian threefold defined over a field  $K$  with  $\text{char } K \neq 2$ . Assume that  $a$  is geometrically indecomposable. There exists a unique primitive geometric Siegel modular form of weight 18 defined over  $\mathbb{Z}$ , denoted  $\chi_{18}$ , such that*

- i)  $(A, a)$  is a hyperelliptic Jacobian if and only if  $\chi_{18}(A, a) = 0$ .
- ii)  $(A, a)$  is a non hyperelliptic Jacobian if and only if  $\chi_{18}(A, a)$  is a non-zero square.

Moreover, if  $K \subset \mathbb{C}$ , let

- $(\omega_1, \omega_2, \omega_3)$  be a basis of regular differentials on  $A$ ;
- $\gamma_1, \dots, \gamma_6$  be a symplectic basis (for  $a$ ) of  $H_1(A, \mathbb{Z})$ ;
- $\Omega_a := [\Omega_1 \ \Omega_2] = [\int_{\gamma_j} \omega_i]$  be a period matrix with  $\tau_a := \Omega_2^{-1} \Omega_1 \in \mathbb{H}_3$  a Riemann matrix.

Then  $(A, a)$  is a Jacobian if and only if

$$(2) \quad \chi_{18}((A, a), \omega_1 \wedge \omega_2 \wedge \omega_3) := \frac{(2\pi)^{54}}{2^{28}} \cdot \frac{\prod_{[\varepsilon]} \theta[\varepsilon](\tau_a)}{\det(\Omega_2)^{18}}$$

is a square in  $K$ .

Let us recall that the *Thetanullwerte*  $\theta[\varepsilon](\tau)$  are the 36 constants such that

$$[\varepsilon] = \begin{bmatrix} \epsilon_1 \\ \epsilon_2 \end{bmatrix} \in \{0, 1\}^3 \oplus \{0, 1\}^3,$$

with  $\epsilon_1^t \epsilon_2 \equiv 0 \pmod{2}$  and for  $\tau \in \mathbb{H}_3$

$$\theta \begin{bmatrix} \epsilon_1 \\ \epsilon_2 \end{bmatrix} (\tau) = \sum_{n \in \mathbb{Z}^3} \exp(i\pi(n + \epsilon_1/2)\tau^t(n + \epsilon_1/2) + i\pi(n + \epsilon_1/2)^t \epsilon_2).$$

**Remark 5.4.** — For a different approach on this result, see [Mea08].

The initial aim of Serre's letter was of course the existence of optimal curves of genus 3. However, one does not know how to compute directly the value of  $\chi_{18}$  over finite fields. Therefore, as Serre suggested, when  $A$  is ordinary, we lift  $(A, a)$  canonically over a number field and there, we use formula (2). Doing the computation with enough precision, we can

recognize this value as an algebraic number. Finally we reduce it to the initial finite field to see if it is a square.

As the Jacobian of an optimal curve is isogenous to the power of an elliptic curve  $E$ , in [Rit10], we worked out this procedure explicit in the particular case  $A = E^3$ . Let  $a_0$  be the product principal polarization on  $E^3$  and  $M = a_0^{-1}a \in M_3(\text{End}(E))$ . When  $\text{End}(E)$  is an order in an imaginary quadratic field, it is well known that  $M$  is the matrix of a principal polarization on  $E^3$  if and only if  $M$  is a positive definite hermitian matrix with determinant 1 (see Remark 3.2 and [Mum08, p.209]). Moreover, when  $E$  is defined over a number field, we show how to translate the data  $(E^3, a_0M)$  into a period matrix of the corresponding torus in order to compute the analytic expression of  $\chi_{18}$ . Let us illustrate this procedure with the following example.

**Example 5.5.** — Does there exist an optimal curve  $C$  of genus 3 over  $k = \mathbb{F}_{47}$ ? If so, by Lemma 2.4 we know that  $\text{Jac } C$  is isogenous to  $E^3$  where  $E$  is an elliptic curve with trace  $-[2\sqrt{47}] = -13$ . The curve  $E$  is then an ordinary elliptic curve and  $\text{End}(E)$  contains  $\mathbb{Z}[\pi] \simeq \mathbb{Z}[(13 + \sqrt{13^2 - 4 \cdot 47})/2] = \mathbb{Z}[\tau]$  (where  $\pi$  is the  $k$ -Frobenius endomorphism and  $\tau = (1 + \sqrt{-19})/2$ ). Hence  $\text{End}(E) = \mathbb{Z}[\pi]$  is the ring of integers  $\mathcal{O}_L$  of  $L = \mathbb{Q}(\sqrt{-19})$ . Since  $\mathcal{O}_L$  is principal,  $E$  is unique up to isomorphism. Using the work of [Sch98], one can see that, up to automorphism, there is a unique positive definite hermitian matrix  $M \in M_3(\mathcal{O}_L)$  of determinant 1 which is indecomposable. In the language of Section 3.1, this means that there exists a unique positive definite unimodular indecomposable rank 3 hermitian  $\mathcal{O}_L$ -module. The abelian threefold  $(E^3, a_0M)$  is then the unique principally polarized geometrically indecomposable abelian threefold with Weil polynomial  $(X^2 + 13X + 47)^3$ , up to isomorphism. Lifting  $E$  canonically over  $\mathbb{Q}$  as  $\bar{E} : y^2 = x^3 - 152x - 722$  we can consider the principally polarized abelian threefold  $(\bar{E}^3, a_0M)$  since  $\text{End}(\bar{E}) = \mathcal{O}_L$  as well. Let  $[w_1 \ w_2]$  be a period matrix of  $E$  with respect to the canonical regular differential  $dx/(2y)$ . If we let

$$\Omega_0 = \left[ \begin{pmatrix} w_1 & 0 & 0 \\ 0 & w_1 & 0 \\ 0 & 0 & w_1 \end{pmatrix} \begin{pmatrix} w_2 & 0 & 0 \\ 0 & w_2 & 0 \\ 0 & 0 & w_2 \end{pmatrix} \right],$$

$\mathbb{C}^3/\Omega_0\mathbb{Z}^6 \simeq \bar{E}^3(\mathbb{C})$  with the product polarization  $a_0$ . We then need to find a symplectic basis of  $\Omega_0\mathbb{Z}^6$  for the polarization  $a_0M$ . It is not difficult to prove that the first Chern class of  $a_0M$  with respect to the pull-back  $\omega_i$  of the differentials  $dx/(2y)$  on each curve is represented by the matrix

$$H = \frac{1}{w_1\bar{w}_2} {}^tM.$$

The alternated form  $T$  classically associated to  $H$  on the lattice  $\Omega_0\mathbb{Z}^6$  is  $T = \text{Im}({}^t\Omega_0 H \bar{\Omega}_0)$ . One then finds a matrix  $B \in \text{GL}_6(\mathbb{Z})$  such that

$$BT {}^tB = \begin{bmatrix} 0 & \mathbf{I}_3 \\ -\mathbf{I}_3 & 0 \end{bmatrix}$$

and  $\Omega = \Omega_0 {}^tB$  is a period matrix for the polarization  $a_0M$ . Finally, one computes an approximation of

$$\chi = \chi_{18}((\bar{E}^3, a_0M), \omega_1 \wedge \omega_2 \wedge \omega_3)$$

thanks to the analytic formula (2) and we recognize it as an element of  $L$ . We find in our case

$$\chi = (2^{19} \cdot 19^7)^2.$$

The value  $\chi$  is a non-zero square over  $\mathbb{F}_{47}$  so by Theorem 5.3 (ii) Serre's obstruction is trivial and there is a non hyperelliptic optimal curve of genus 3 over  $k$ .

Similar computations show that there is an optimal curve over  $\mathbb{F}_q$  for  $q = 61, 137, 277$  but not for  $q = 311$ . Note that this result for  $q = 47$  and  $q = 61$  has already been obtained in [Top03] using explicit models and the others have been confirmed by [AAMZ09]. In [Rit10], tables of values of  $\chi$  as the one from Example 5.5 are given for  $(\bar{E}^3, a_0M)$  where  $\bar{E}$  is an elliptic curve with class number 1 and  $M$  is taken from [Sch98]. From them, we can get for instance:

**Proposition 5.6.** — *Assume that  $q = p^n$  is such that  $4q = m^2 + d$  with  $d = 7$  (resp. 19). Then there exists an (explicit) genus 3 optimal curve over  $\mathbb{F}_q$  if and only if*

$$m \equiv 1, 2 \text{ or } 4 \pmod{7} \text{ (resp. } \left(\frac{m}{19}\right) \left(\frac{-2}{p}\right) = 1).$$

Moreover if this curve exists, it is non hyperelliptic.

Assume that  $q = p^n$  is such that  $4q = m^2 + 43$ . In particular 43 is a square in  $\mathbb{F}_p$ , let say  $43 = r^2$  with  $r \in \mathbb{F}_p$ . Then there exists a genus 3 optimal curve over  $\mathbb{F}_q$  if and only if

$$\left(\frac{m}{43}\right) \left(\frac{\alpha}{p}\right) = 1$$

where  $\alpha$  is either  $-2 \cdot 3 \cdot 7, -487, -47 \cdot 79 \cdot 107 \cdot 173$  or  $-15156 \pm 8214r$ . Moreover if this curve exists, it is non hyperelliptic.

**Remark 5.7.** — The term ‘explicit’ in Proposition 5.6 comes from the fact that for certain  $(\bar{E}^3, a_0M)$  of [Rit10] we were able to give the equation of a curve  $\bar{C}$  such that  $\text{Jac } \bar{C}$  is isomorphic to  $(\bar{E}^3, a_0M)$  using [Guà09]. Hence for these cases, we have a ‘universal’ family of explicit equations for the optimal curve.

The fact that the previous statement is embarrassingly cumbersome reveals either the intrinsic difficulty of the problem or a wrong attack angle. Moreover, the limits of this strategy already appear in the example: the computation of the canonical lift, of the matrices  $M$  and of a period matrix make it algorithmic in nature. Worse, the computation of an approximation of  $\chi$  is time-consuming since one has to recognize it as an algebraic number (actually for a good choice of the model  $\bar{E}$ ,  $\chi$  is an algebraic integer). Therefore large values of the discriminant of  $\text{End}(E)$  seem out of reach.

It might then be interesting to try to understand the prime decomposition of  $\chi$  algebraically. Klein's formula linking  $\chi_{18}$  to the square of the discriminant of plane quartics (see [Kle90, Eq.118, p.462] and [LRZ10, Th.2.23]) makes us think about an analogue of the Néron-Ogg-Shafarevich formula for elliptic curve [Sil92, Appendix C, 16]. We shall then interpret  $\mathfrak{p}|\chi$  in terms of the nature of  $(A, a) := (\bar{E}^3, a_0M) \pmod{\mathfrak{p}}$ . For instance, using [Ich95, p.1059],  $\mathfrak{p}|\chi$  if and only if  $(A, a)$  is geometrically decomposable or a hyperelliptic Jacobian. Unfortunately, we do not know how to detect algebraically this last possibility (see the discussion in [Rit09, Sec.4.5.1]).

**Remark 5.8.** — We have not spoken yet about the case  $q$  square when  $p > 2$ . First, when  $p \equiv 3 \pmod{4}$ , one knows [Ibu93, p.2] that there exists an optimal genus 3 curve. This curve is even hyperelliptic [Oor91] but not explicit (see however [KTW09] for some explicit sub-cases). Also Fermat curve  $x^4 + y^4 + z^4 = 0$  is optimal if  $n \equiv 2 \pmod{4}$ . Then, when  $p \equiv 1 \pmod{4}$  and  $n \equiv 2 \pmod{4}$ , Ibukiyama (*loc. cit.*) shows that there is an optimal curve. Ibukiyama's strategy uses a mass formula on quaternion hermitian forms to show the descent of an indecomposable principal polarization on a model over  $\mathbb{F}_p$  of  $E^3$  where  $E/\mathbb{F}_{p^2}$  is an elliptic curve with trace  $-2p = -m$ . The abelian threefold and its quadratic twist being isomorphic over  $\mathbb{F}_{p^2}$ , he avoids the issue of computing Serre's obstruction.

**5.3. The geometric approach.** — Following a construction of Recillas [Rec74], we were able to give in [BR10] a geometric characterization of Serre's obstruction. For the sake of simplicity, let us assume that  $\text{char } k \neq 2$  and that  $(A, a)/k$  is geometrically the Jacobian of a non hyperelliptic genus 3 curve. Since  $k$  is a finite field, there exists a symmetric theta divisor  $\Theta$  (for the polarization  $a$ ) defined over  $k$ . Let  $\Sigma$  be the union of  $2_*\Theta$  and of the unique divisor in  $|2\Theta|$  with multiplicity greater than or equal to 4 at 0.

**Proposition 5.9.** — *Let  $\alpha \in A(\bar{k}) \setminus \{0\}$ . The curve  $\tilde{X}_\alpha = \Theta \cap (\Theta + \alpha)$  is smooth and connected if and only if  $\alpha \in A(\bar{k}) \setminus \Sigma$ .*

Hence, the divisor  $\Sigma$  represents a bad locus that needs to be avoided in the sequel. Assuming that  $\alpha \notin \Sigma$ , the involution  $(z \mapsto \alpha - z)$  of  $\tilde{X}_\alpha$  is fixed point free and so  $X_\alpha = \tilde{X}_\alpha / (z \mapsto \alpha - z)$  is a smooth genus 4 curve.

**Proposition 5.10.** — *The curve  $X_\alpha$  is non hyperelliptic and its canonical model in  $\mathbb{P}^3$  lies on a quadric  $Q_\alpha$  which is smooth.*

To go further, we need to assume that  $\alpha$  is rational. When  $k$  is big enough, such an  $\alpha$  always exists. We then obtain the following result.

**Theorem 5.11.** — *Assume there exists  $\alpha \in A(k) \setminus \Sigma$ . Then  $(A, a)$  is a Jacobian if and only if  $\delta = \text{Disc } Q_\alpha$  is a square in  $k^*$ .*

Let us sketch the proof. A non hyperelliptic genus 4 curve  $X$  lies canonically in  $\mathbb{P}^3$  on the intersection of a unique quadric  $Q$  and a cubic surface  $E$ . If we assume that  $Q$  is smooth, then  $X$  has two  $g_3^1$  coming from the two rulings of  $Q$  by intersecting them with  $E$ . Moreover, an easy computation shows that  $\text{Disc } Q$  is a square if and only if these two  $g_3^1$  are defined over  $k$ . Now Recillas' construction, which can be used when  $(A, a)$  is the Jacobian of a curve, shows that  $X_\alpha$  has two (rather explicit) rational  $g_3^1$ . To conclude, it is then enough to show that a quadratic twist of  $(A, a)$  (which is no more a Jacobian) leads to two conjugate  $g_3^1$ .

The advantage of this approach is that it stays over the finite field  $k$  and is completely algebraic. Unfortunately, so far, we do not see how to compute  $\delta$  for  $A = E^3$  and  $a = a_0M$  in terms of an equation of  $E$  and the coefficients of  $M$ . The main difficulty seems to find an equation (or even points) on a theta divisor in order to compute an equation of  $Q_\alpha$ .

## References

- [AAMZ09] E. Alekseenko, S. Aleshnikov, N. Markin, and A. Zaytsev. Optimal curves of genus 3 over finite fields with discriminant -19, 2009. Available on <http://www.citebase.org/abstract?id=oai:arXiv.org:0902.1901>.
- [BHV01] Yu. Bilu, G. Hanrot, and P. M. Voutier. Existence of primitive divisors of Lucas and Lehmer numbers. *J. Reine Angew. Math.*, 539:75–122, 2001. With an appendix by M. Mignotte.
- [BR10] Arnaud Beauville and Christophe Ritzenthaler. Jacobians among abelian threefolds: a geometric approach, 2010. to appear in *Math. Annal.*
- [Bro93] Bradley W. Brock. *Superspecial curves of genera two and three*. PhD thesis, Princeton university, Princeton, 1993.
- [Del69] Pierre Deligne. Variétés abéliennes ordinaires sur un corps fini. *Invent. Math.*, 8:238–243, 1969.
- [Deu41] Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941.
- [Dic66] Leonard Eugene Dickson. *History of the theory of numbers. Vol. II: Diophantine analysis*. Chelsea Publishing Co., New York, 1966.
- [Eke87] Torsten Ekedahl. On supersingular curves and abelian varieties. *Math. Scand.*, 60(2):151–178, 1987.
- [Gop77] Valerii Denisovich Goppa. Codes that are associated with divisors. *Problemy Peredači Informacii*, 13(1):33–39, 1977.
- [Gop88] Valerii Denisovich Goppa. *Geometry and codes*, volume 24 of *Mathematics and its Applications (Soviet Series)*. Kluwer Academic Publishers Group, Dordrecht, 1988. Translated from the Russian by N. G. Shartse.
- [Guà09] Jordi Guàrdia. On the Torelli problem and jacobian nullwerte in genus three, 2009. <http://arxiv.org/abs/0901.4376>.
- [Hal10] Safia Haloui. The characteristic polynomials of abelian varieties of dimensions 3 over finite fields. *J. Number Theory*, 130:2745–2752, 2010.
- [Has83] Ki-ichiro Hashimoto. Class numbers of positive definite ternary quaternion Hermitian forms. *Proc. Japan Acad. Ser. A Math. Sci.*, 59(10):490–493, 1983.
- [Hay68] Tsuyoshi Hayashida. A class number associated with the product of an elliptic curve with itself. *J. Math. Soc. Japan*, 20:26–43, 1968.
- [HI83] Ki-ichiro Hashimoto and Tomoyoshi Ibukiyama. On class numbers of positive definite binary quaternion Hermitian forms. I,II,III. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 27,28,30:549–601, 695–699,393–401, 1980,1981,1983.
- [HK86] Ki-ichiro Hashimoto and Harutaka Koseki. Class numbers of positive definite binary and ternary unimodular Hermitian forms. *Proc. Japan Acad. Ser. A Math. Sci.*, 62(8):323–326, 1986.
- [HK89] Ki-ichiro Hashimoto and Harutaka Koseki. Class numbers of positive definite binary and ternary unimodular Hermitian forms. *Tohoku Math. J. (2)*, 41(2):171–216, 1989.
- [HLP00] Everett W. Howe, Franck Leprévost, and Bjorn Poonen. Large torsion subgroups of split Jacobians of curves of genus two or three. *Forum Math.*, 12(3):315–364, 2000.
- [HN65] Tsuyoshi Hayashida and Mieno Nishi. Existence of curves of genus two on a product of two elliptic curves. *J. Math. Soc. Japan*, 17:1–16, 1965.
- [HNR09] Everett W. Howe, Enric Nart, and Christophe Ritzenthaler. Jacobians in isogeny classes of abelian surfaces over finite fields. *Annales de l’institut Fourier*, 59:239–289, 2009.

- [Hof91] Detlev W. Hoffmann. On positive definite Hermitian forms. *Manuscripta Math.*, 71(4):399–429, 1991.
- [Hon68] Taira Honda. Isogeny classes of abelian varieties over finite fields. *J. Math. Soc. Japan*, 20:83–95, 1968.
- [How95] Everett W. Howe. Principally polarized ordinary abelian varieties over finite fields. *Trans. Amer. Math. Soc.*, 347(7):2361–2401, 1995.
- [How96] Everett W. Howe. Kernels of polarizations of abelian varieties over finite fields. *J. Algebraic Geom.*, 5(3):583–608, 1996.
- [How08] Everett W. Howe. Supersingular genus-2 curves over fields of characteristic 3. In *Computational arithmetic geometry*, volume 463 of *Contemp. Math.*, pages 49–69. Amer. Math. Soc., Providence, RI, 2008.
- [Ibu89] Tomoyoshi Ibukiyama. On automorphism groups of positive definite binary quaternion Hermitian lattices and new mass formula. In *Automorphic forms and geometry of arithmetic varieties*, volume 15 of *Adv. Stud. Pure Math.*, pages 301–349. Academic Press, Boston, MA, 1989.
- [Ibu93] Tomoyoshi Ibukiyama. On rational points of curves of genus 3 over finite fields. *Tohoku Math. J. (2)*, 45(3):311–329, 1993.
- [Ich95] Takashi Ichikawa. Teichmüller modular forms of degree 3. *Amer. J. Math.*, 117(4):1057–1061, 1995.
- [Igu67] Jun-ichi Igusa. Modular forms and projective invariants. *Amer. J. Math.*, 89:817–855, 1967.
- [IKO86] Tomoyoshi Ibukiyama, Toshiyuki Katsura, and Frans Oort. Supersingular curves of genus two and class numbers. *Compositio Math.*, 57(2):127–152, 1986.
- [Kan97] Ernst Kani. The number of curves of genus two with elliptic differentials. *J. Reine Angew. Math.*, 485:93–121, 1997.
- [Kle90] Felix Klein. Zur Theorie der Abelschen Funktionen. *Math. Annalen*, 36:388–474, 1889–90. =Gesammelte mathematische Abhandlungen, XCVII, 388–474.
- [KO87] Toshiyuki Katsura and Frans Oort. Supersingular abelian varieties of dimension two or three and class numbers. In *Algebraic geometry, Sendai, 1985*, volume 10 of *Adv. Stud. Pure Math.*, pages 253–281. North-Holland, Amsterdam, 1987.
- [KTW09] Tetsuo Kodama, Jaap Top, and Tadashi Washio. Maximal hyperelliptic curves of genus three. *Finite Fields Appl.*, 15(3):392–403, 2009.
- [Kuh88] Robert M. Kuhn. Curves of genus 2 with split Jacobian. *Trans. Amer. Math. Soc.*, 307(1):41–49, 1988.
- [Lan06] Herbert Lange. Principal polarizations on products of elliptic curves. In *The geometry of Riemann surfaces and abelian varieties*, volume 397 of *Contemp. Math.*, pages 153–162. Amer. Math. Soc., Providence, RI, 2006.
- [Lau02] Kristin Lauter. The maximum or minimum number of rational points on genus three curves over finite fields. *Compositio Math.*, 134(1):87–111, 2002. With an appendix by Jean-Pierre Serre.
- [LR08] Gilles Lachaud and Christophe Ritzenthaler. On some questions of Serre on abelian threefolds. In *Algebraic geometry and its applications*, volume 5 of *Ser. Number Theory Appl.*, pages 88–115. World Sci. Publ., Hackensack, NJ, 2008.
- [LRZ10] Gilles Lachaud, Christophe Ritzenthaler, and Alexey Zykin. Jacobians among abelian threefolds: a formula of Klein and a question of Serre. *Math. Res. Lett.*, 17(2), 2010.
- [Mat58] Teruhisa Matsusaka. On a theorem of Torelli. *Amer. J. Math.*, 80:784–800, 1958.
- [Maz86] Barry Mazur. Arithmetic on curves. *Bull. Amer. Math. Soc. (N.S.)*, 14(2):207–259, 1986.



- [Mea08] Stephen Meagher. *Twists of genus 3 and their Jacobians*. PhD thesis, Rijksuniversiteit Groningen, 2008.
- [Mes10] Jean-François Mestre. Courbes de genre 3 avec  $S_3$  comme groupe d'automorphismes, 2010. <http://arxiv.org/abs/1002.4751>.
- [MN02] Daniel Maisner and Enric Nart. Abelian surfaces over finite fields as jacobians. *Experimental Math.*, 11:321–337, 2002. with an appendix of E.W. Howe.
- [MN07] Daniel Maisner and Enric Nart. Zeta functions of supersingular curves of genus 2. *Canad. J. Math.*, 59(2):372–392, 2007.
- [Mum08] David Mumford. *Abelian varieties*, volume 5 of *Tata Institute of Fundamental Research Studies in Mathematics*. Published for the Tata Institute of Fundamental Research, Bombay, 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition.
- [MW71] James Stuart Milne and William C. Waterhouse. Abelian varieties over finite fields. 1969 Number Theory Institute, Proc. Sympos. Pure Math. 20, 53–64, 1971.
- [NR08] Enric Nart and Christophe Ritzenthaler. Jacobians in isogeny classes of supersingular abelian threefolds in characteristic 2. *Finite fields and their applications*, 14:676–702, 2008.
- [NR10] Enric Nart and Christophe Ritzenthaler. Genus three curves with many involutions and application to maximal curves in characteristic 2. In *Proceedings of AGCT-12*, volume 521, pages 71–85. Contemporary Mathematics, 2010.
- [Oor75] Frans Oort. Which abelian surfaces are products of elliptic curves? *Math. Ann.*, 214:35–47, 1975.
- [Oor91] Frans Oort. Hyperelliptic supersingular curves. In *Arithmetic Algebraic Geometry (Texel, 1989)*, Prog. Math., pages 247–284, Boston, 1991. Birkhäuser.
- [OU73] Frans Oort and Kenji Ueno. Principally polarized abelian varieties of dimension two or three are Jacobian varieties. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 20:377–381, 1973.
- [Rec74] Sevin Recillas. Jacobians of curves with  $g_4^1$ 's are the Prym's of trigonal curves. *Bol. Soc. Mat. Mexicana (2)*, 19(1):9–13, 1974.
- [Rit09] Christophe Ritzenthaler. *Aspects arithmétiques et algorithmiques des courbes de genre 1, 2 et 3*. Habilitation à Diriger des Recherches, Université de la Méditerranée, 2009.
- [Rit10] Christophe Ritzenthaler. Explicit computations of Serre's obstruction for genus-3 curves and application to optimal curves. *LMS J. Comput. Math.*, 13:192–207, 2010.
- [Ryb08] Sergey Rybakov. *Zeta functions of algebraic surfaces and Jacobians of genus 3 curves over finite fields*. PhD thesis, Moscow State University, Mechanics and Math. Department, 2008. in russian, unpublished.
- [Sch98] Alexander Schiemann. Classification of Hermitian forms with the neighbour method. *J. Symbolic Comput.*, 26(4):487–508, 1998. tables available on <http://www.math.uni-sb.de/ag/schulze/Hermitian-lattices/>.
- [Sek86] Tsutomu Sekiguchi. Erratum: “On the fields of rationality for curves and for their Jacobian varieties” [Nagoya Math. J. **88** (1982), 197–212; MR0683250 (85a:14021)]. *Nagoya Math. J.*, 103:163, 1986.
- [Ser68] Jean-Pierre Serre. *Corps locaux*. Hermann, Paris, 1968. Deuxième édition, Publications de l'Université de Nancago, No. VIII.
- [Ser83a] Jean-Pierre Serre. Nombres de points des courbes algébriques sur  $\mathbf{F}_q$ . In *Seminar on number theory, 1982–1983 (Talence, 1982/1983)*, pages Exp. No. 22, 8. Univ. Bordeaux I, Talence, 1983.

- 
- [Ser83b] Jean-Pierre Serre. Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini. *C. R. Acad. Sci. Paris Sér. I Math.*, 296(9):397–402, 1983.
- [Ser85] Jean-Pierre Serre. Rational points on curves over finite fields, 1985. Lectures given at Harvard, notes by F.Q. Gouvêa.
- [Sha01] Vasily Shabat. *Curves with many points*. PhD thesis, Universiteit van Amsterdam, Amsterdam, 2001.
- [Shi79] Tetsuji Shioda. Supersingular  $K3$  surfaces. In *Algebraic geometry (Proc. Summer Meeting, Univ. Copenhagen, Copenhagen, 1978)*, volume 732 of *Lecture Notes in Math.*, pages 564–591. Springer, Berlin, 1979.
- [Sil92] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.
- [Tat66] John Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.
- [Tat71] John Tate. Classes d'isogénie des variétés abéliennes sur un corps fini (d'après Honda). In *Séminaire Bourbaki 1968/69*, volume 179 of *Lecture Notes in Math.*, pages 95–110. Springer, Berlin, 1971.
- [Top03] Jaap Top. Curves of genus 3 over small finite fields. *Indag. Math. (N.S.)*, 14(2):275–283, 2003.
- [Wat69] William C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)*, 2:521–560, 1969.
- [Wei48] André Weil. *Variétés abéliennes et courbes algébriques*. Actualités Sci. Ind., no. 1064 = Publ. Inst. Math. Univ. Strasbourg 8 (1946). Hermann & Cie., Paris, 1948.
- [WL01] Rui Qing Wang and Guo Sheng Li. Indecomposable definite Hermitian forms over imaginary quadratic fields. *J. Zhengzhou Univ. Nat. Sci. Ed.*, 33(3):22–27, 2001.
- [Xin96] Chaoping Xing. On supersingular abelian varieties of dimension two over finite fields. *Finite Fields Appl.*, 2(4):407–421, 1996.
- [Zhu97] Fu-Zu Zhu. On the construction of indecomposable positive definite Hermitian forms over imaginary quadratic fields. *J. Number Theory*, 62(2):353–367, 1997.

---

12 octobre 2010

CHRISTOPHE RITZENTHALER, Institut de Mathématiques de Luminy, UMR 6206 du CNRS, Luminy, Case 907, 13288 Marseille, France. • E-mail : [ritzenth@iml.univ-mrs.fr](mailto:ritzenth@iml.univ-mrs.fr)